歪多項式環の平田分離多項式について (代数と言語のアルゴリズムと計算理論)

AUTHOR(S):

池畑, 秀一

CITATION:

池畑, 秀一. 歪多項式環の平田分離多項式について (代数と言語のアルゴリズムと計算理論). 数理解析研究所講究録 2010, 1712: 76-82

ISSUE DATE:

2010-09

URL:

http://hdl.handle.net/2433/170235

数理解析研究所講究録
第1712巻 2010年 76-82

歪多項式環の平田分離多項式について

岡山大学・大学院自然科学研究科　池畑　秀一 (Shûichi IKEHATA)
Graduate School of Natural Science and Technology
Okayama University

1. 序と準備

本論を通して, B は単位元1を持つ環とし, Z は B の中心, ρ を B の自己同型写像, D は B の ρ-微分 (ρ-derivaiton) とする. すなわち, D は B から B への加法的写像で $D(\alpha\beta)=\alpha D(\beta)+D(\alpha)\rho(\beta)$ $(\alpha,\beta\in B)$ を満たすものとする. $B[X;\rho,D]$ をその乗法が $\alpha X=X\rho(\alpha)+D(\alpha)$ $(\alpha\in B)$ によって定まる歪多項式環とする. 環の拡大 A/B が分離拡大 (separable extension) であるとは $A\otimes_B A$ から A への A-A-準同型写像 $a\otimes b\to ab$ が分解 (splits) することである. また A/B が平田分離拡大 (Hirata separable extension) であるとは $A\otimes_B A$ が A の有限個の直和の直和因子に A-A-同型であることである. 良く知られているように平田分離拡大は分離拡大である. 平田分離拡大は, 平田和彦が1968年に [1] で, 東屋多元環の一般化として初めて導入した概念である. 平田分離拡大はこれまで H-分離拡大と呼ばれてきたが, 最近 G. Szeto と L. Xue が初めて考察した平田和彦にちなんで Hirata separable extension (平田分離拡大) と呼び始めたので, 筆者もそれにならうことにする. これまで使われていた H-分離拡大という呼称は菅野孝三が平田の頭文字 H をとって名付けたものである. 菅野孝三は2004年に亡くなるまで一貫して平田分離拡大の研究を続けた. 最近, 作用素環論などの分野で平田分離拡大やそれに類する環拡大が現れ, その重要性が注目されるようになってきた. 本稿の目的は歪多項式環のモニックな多項式によって生成されるイデアルの剰余環として現れる環拡大で平田分離拡大となっているものについての最近の結果を紹介することである.

f を歪多項式環 $B[X;\rho,D]$ のモニックな多項式で $fB[X;\rho,D]=B[X;\rho,D]f$ を満たすものとする. このとき剰余環 $B[X;\rho,D]/fB[X;\rho,D]$ は B の free な拡大環となる.

$B[X;\rho,D]/fB[X;\rho,D]$ が B 上分離拡大 (resp. 平田分離拡大) のとき,
f を歪多項式環 $B[X;\rho,D]$ における分離多項式 (resp. 平田分離多項式) という.

$D=0$ の場合を自己同型型といい $B[X;\rho,0]=B[X;\rho]$ と表し, $\rho=1_B$ の場合を微分型といい $B[X;1_B,D]=B[X;D]$ と表す. 一般の場合は極めて計算が困難であるからまずこれら2つの場合に調べるのが常である. これら歪多項式環の剰余環として現れる拡大は分離拡大や平田分離拡大の典型的な, また本質的な例を与える.

これまでの研究の歴史を簡単に振り返ってみる. 岸本量男は1970年代に [16, 17, 18] で, $B[X;\rho]$ における X^m-u や $B[X;D]$ における X^p-X-b などの特別なタイプの多項式の分離性やガロア性について論じた. 永原賢は [21] およびそれに続く一連の論文で歪多項式環における2次の分離多項式やガロア多項式について徹底的な研究を行った. 宮下庸一は [20] で, $*$-positively filtered ring の一般論を展開することにより, その応用として一般次数の多項式の研究を可能にした. 筆者は宮下庸一の方法を用いて [4, 5] およびそれに続く一連の論文で歪多項式環における一般次数の分離多項式や平田分離多項式について研究した. そこでわかったことは平田分離多項式の存

在は極めて強い条件であるということである.次の節でこれまでに知られている平田分離多項式に関する性質をまとめておく.

2. 平田分離多項式についての既知の結果

命題 2.1. ([5, Proposition 1.2]) $B[X;\rho]$ が次数 m の平田分離多項式 f を含めば, 必然的に $f = X^m - u$ という形をしている.

命題 2.2. ([5, Theorems 2.1, 2.2]) B を可換環とし, $B[X;\rho]$ が $f = X^m - u$ を含み, $fB[X;\rho] = B[X;\rho]f$ を満たすものとする. $S = B[X;\rho]/fB[X;\rho]$, $A = B^\rho$ とおくとき, 次は同値である.

(1) f は平田分離多項式である.

(2) S は東屋 A-多元環である.

(3) B/A は $<\rho>$ -ガロア拡大で,$<\rho>$ の次数は m であり,u は B^ρ の可逆元である.

このとき,$B[X;\rho]$ の平田分離多項式全体の集合は $\{X^m + c \mid c \text{ は } B^\rho \text{ の可逆元}\}$ である.

上の結果が B が非可換環のときにどうなるかを考えるのは自然である.2000 年に G. Szeto と L. Xue が次の結果を得た.

命題 2.3. ([25, Theorem 3.6]) $B[X;\rho]$ が $f = X^m - u$ を含み, $fB[X;\rho] = B[X;\rho]f$ を満たすものとする. このとき次は同値である.

(1) f は平田分離多項式である.

(2) Z/Z^ρ は $<\rho|Z>$-ガロア拡大で,$<\rho|Z>$ の次数は m であり,u は B^ρ の可逆元である.

上の命題で,(2) $\Rightarrow$ (1) は B が非可換の場合でも容易に成り立つことがわかるが, (1) $\Rightarrow$ (2) を示すことが容易でない部分であり, 筆者は m が素数のときのみ [7] で証明していた.G. Szeto と L. Xue が一般の場合に, F. DeMeyer の「巡回ガロア多元環は可換環である」という定理を用いて証明に成功した.

上の定理により, 自己同型型の歪多項式環 $B[X;\rho]$ が平田分離多項式を含むための必要十分条件は B の中心 Z が Z^ρ 上の $<\rho|Z>$-ガロア拡大であるということで特徴付けられたことになる.

次に微分型歪多項式環においてはどうなっているだろうか.

命題 2.4. ([10, Theorem 2.2]) もし $B[X;D]$ が次数 $m \geq 2$ の平田分離多項式 f を含めば, 次が成り立つ:

(1) B は必然的に素数標数 p となり f は次のような p-多項式の形をしている.

$$f = X^{p^e} + X^{p^{e-1}}\alpha_e + \cdots + X^p\alpha_2 + X\alpha_1 + \alpha_0,$$

ここで, $m = p^e$ であり $\alpha_j \in Z^D$ $(1 \leq j \leq e)$, $\alpha_0 \in B^D$.

(2) $B[X;D]$ の中心は $Z^D[f]$ と一致する, すなわち, $V_{B[X;D]}(B[X;D]) = Z^D[f]$.

(3) $B[X;D]$ のすべての平田分離多項式は $f + c$ の型をしている, ここで c は Z^D の元である.

上の結果は, 微分型歪多項式環においても平田分離多項式が存在するという条件は, 極めて強い条件であることを示している. 以後は微分型歪多項式環のみを取り扱うので, B は素数標数 p であると仮定することにする.

係数環 B が可換環のときには命題2.2に対応する結果として次が成りたつ.

命題 2.5. ([5, Theorems 3.1, 3.3]) B を可換環とし, $B[X;D]$ が $f = X^{p^e}+X^{p^{e-1}}\alpha_e+\cdots+X^p\alpha_2+X\alpha_1+\alpha_0$ を含み, $fB[X;D] = B[X;D]f$ を満たすものとする. $S = B[X;D]/fB[X;D]$, $A = B^D$ とおくとき, 次は同値である.

(1) f は平田分離多項式である.

(2) S は東屋 A-多元環である.

(3) 適当な元 $y_i, z_i \in B$ が存在して

$$\sum_i D^{p^e-1}(y_i)z_i = 1, \quad \sum_i D^k(y_i)z_i = 0 \ \ (0 \le k \le p^e-2)$$

が成り立つ.

(4) ${}_AB$ は階数 p^e の有限生成射影加群で, $\mathrm{Hom}({}_AB, {}_AB) = B[D]$ となる. (これは B/A が S. Yuan の意味の指数1の純非分離拡大ということである).

上の結果を係数環 B が非可換環のときに拡張しようと試みてきた. B を非可換環とするとき命題2.3に対応する結果が成り立つことを期待することは自然であると思う. まず次は成り立つ.

命題 2.6. ([10, Proposition 2.3]) B を環とし Z をその中心, D を B の微分とし, $\delta = D|Z$ とする. Z/Z^δ が指数1の純非分離拡大で, ${}_{Z^\delta}Z$ は階数 p^e の射影加群とし, δ が最小多項式 $t^{p^e}+t^{p^{e-1}}\alpha_e+\cdots+t^p\alpha_2+t\alpha_1(\alpha_i \in Z^\delta)$ を満たすと仮定する. もし $D^{p^e}+\alpha_eD^{p^{e-1}}+\cdots+\alpha_2D^p+\alpha_1D = I_u$ を満たす $u \in B^D$ が存在すれば, $f = X^{p^e}+X^{p^{e-1}}\alpha_e+\cdots+X^p\alpha_2+X\alpha_1-u$ は $B[X;D]$ における平田分離多項式である. ここで I_u は u で定まる B の内部微分を表す.

上の命題の逆, すなわち $B[X;D]$ が平田分離多項式を含めば Z が Z^D の上で純非分離拡大であるかということに関しては, 現在のところまだ証明できていない. [13] において多項式 $f = X^p - Xa - b$ で, さらに係数環 B の中心 Z が半素環のときには成立することを示した. しかし一般の次数では半素環の場合ですらまだ解決していない.

なお [10, 11] において, 係数環 B が東屋 Z-多元環の場合に考察した. 例えば次の結果は B が東屋 Z-多元環のときは命題2.6における $u \in B^D$ が必ず取れることを保証している.

命題 2.7. ([11, Theorem 2]) B を東屋 Z-多元環, D を B の微分, $\delta = D|Z$ とする. Z/Z^δ が指数1の純非分離拡大で, ${}_{Z^\delta}Z$ が階数 p^e の射影加群で, δ が最小多項式

$$t^{p^e}+t^{p^{e-1}}\alpha_e+\cdots+t^p\alpha_2+t\alpha_1(\alpha_i \in Z^\delta)$$

を満たすとする. そのとき, B^D の元 u が存在して

$$D^{p^e}+\alpha_eD^{p^{e-1}}+\cdots+\alpha_2D^p+\alpha_1D = I_u.$$

がなりたつ.

3. 主要結果

$B[X;D]$ が平田分離多項式を含めば Z が Z^D の上で純非分離拡大であるかということに関して, 条件 $B = B^D Z$ を満たせば成りたつ. すなわち

定理 3.1. B を環とし Z をその中心, D を B の微分とし, $\delta = D|Z$ とする. $B = B^D Z$ が成り立つものとする. $B[X;D]$ が平田分離多項式 $f = X^{p^e} + X^{p^{e-1}}\alpha_e + \cdots + X^p\alpha_2 + X\alpha_1 + \alpha_0$ を含めば, Z/Z^δ が指数 1 の純非分離拡大で, ${}_{Z^\delta}Z$ は階数 p^e の射影加群となる. このとき,$\alpha_0 \in Z^\delta$ となり, f は $Z[X;\delta]$ の平田分離多項式でもある.
さらに $B[X;D]$ における平田分離多項式の全体と $Z[X;\delta]$ における平田分離多項式の全体は一致し $\{f + c \mid c \in Z^\delta\}$ である.

B が可換環のときは,$B = Z$ であるから, 条件 $B = B^D Z$ は自明に成り立っている. B が非可換のときには, 条件 $B = B^D Z$ はいつも成り立つわけではないし, α_0 が Z でとれるとも限らない. したがって, 問題の解決にはいたっていない. 逆に次も成りたつ.

定理 3.2. B を環とし Z をその中心, D を B の微分とし, $\delta = D|Z$ とする. Z/Z^δ が指数 1 の純非分離拡大で, ${}_{Z^\delta}Z$ は階数 p^e の射影加群とし,δ が最小多項式 $t^{p^e} + t^{p^{e-1}}\alpha_e + \cdots + t^p\alpha_2 + t\alpha_1 (\alpha_i \in Z^\delta)$ を満たすと仮定する. もし $D^{p^e} + \alpha_e D^{p^{e-1}} + \cdots + \alpha_2 D^p + \alpha_1 D = 0$ ならば次が成り立つ.
(1) $B = B^D Z = B^D \otimes_{Z^\delta} Z$, ${}_{B^D}B_{B^D}$ は中心的射影加群で $V_B(B^D) = Z$ が成り立つ.
(2) $\mathrm{Hom}({}_{B^D}B_{B^D}, {}_{B^D}B_{B^D}) = Z[D] = Z \oplus ZD \oplus ZD^2 \oplus \cdots \oplus ZD^{p^e-1}$.
(3) $\mathrm{Der}_{B^D}(B) = ZD \oplus ZD^p \oplus \cdots \oplus ZD^{p^{e-1}}$. とくに,
$\mathrm{Der}_{Z^\delta}(Z) = Z\delta \oplus Z\delta^p \oplus \cdots \oplus Z\delta^{p^{e-1}}$.
(4) $Z[X;\delta]$ は東屋 $Z^\delta[f]$-多元環で $B[X;D] = Z[X;\delta] \otimes_{Z^\delta} B^D$
$= Z[X;\delta] \otimes_{Z^\delta[f]} B^D[f]$, ここで $f = X^{p^e} + X^{p^{e-1}}\alpha_e + \cdots + X^p\alpha_2 + X\alpha_1$.

証明. 写像 $\tau : B \to B$ をつぎのように定義する.

$$\tau(b) = \sum_{j=0}^{e} \alpha_{j+1} D^{p^j - 1}(b).$$

$D^{p^e} + \alpha_e D^{p^{e-1}} + \cdots + \alpha_2 D^p + \alpha_1 D = 0$ であるから, τ は $B^D - B^D$ 写像で, その像は B^D に含まれる. Z/Z^δ が指数 1 の純非分離拡大であるから,[5, Theorem 3.3(d)] により,

$$\sum_i \delta^{p^e-1}(x_i)y_i = 1 \text{ かつ } \sum_i \delta^k(x_i)y_i = 0 \ (0 \le k \le p^e - 2)$$

となる元 $x_i, y_i \in Z$ が存在する. 写像 $\varphi_i : B \to B^D$ を $\varphi_i = \tau(x_i)_r$ によって定義する. そのとき

$$\begin{aligned}\sum_i \varphi_i(b)y_i &= \sum_i \tau(bx_i)y_i \\ &= \sum_i \sum_{j=0}^{e} \alpha_{j+1} D^{p^j-1}(bx_i)y_i \\ &= \sum_i \sum_{j=0}^{e} \alpha_{j+1} \sum_{\nu=0}^{p^j-1} \binom{p^j-1}{\nu} D^{p^j-1-\nu}(b)\delta^\nu(x_i)y_i \\ &= \sum_{j=0}^{e} \alpha_{j+1} \sum_{\nu=0}^{p^j-1} \binom{p^j-1}{\nu} D^{p^j-1-\nu}(b)(\sum_i \delta^\nu(x_i)y_i) \\ &= b \quad (b \in B).\end{aligned}$$

これは $B = B^D Z$ となることを示している. よって $V_B(B^D) = Z$ となり, ${}_{B^D}B_{B^D}$ が中心的射影加群であることもわかる. これで (1) の証明が終わった.
(2) $\varphi \in \mathrm{Hom}({}_{B^D}B_{B^D}, {}_{B^D}B_{B^D})$ とする. そのとき

$$\varphi(b) = \sum_i \tau(bx_i)\varphi(y_i) \quad (b \in B)$$

が成りたつ. $V_B(B^D) = Z$ であるから,$\varphi(Z) \subset Z$ となることがわかる. よって

$$\begin{aligned}\varphi(b) &= \sum_i \varphi(y_i)\tau(bx_i) \\ &= \sum_i \varphi(y_i) \sum_{j=0}^{e} \alpha_{j+1} \sum_{\nu=0}^{p^j-1} \binom{p^j-1}{\nu} \delta^{p^j-1-\nu}(x_i) D^\nu(b).\end{aligned}$$

これより $\varphi \in \sum_{\nu=0}^{p^j-1} ZD^\nu$ がわかる. $f = X^{p^e} + X^{p^{e-1}}\alpha_e + \cdots + X^p\alpha_2 + X\alpha_1 - u$ は $B[X;D]$ における平田分離多項式であるから, $1, D, D^2, \cdots, D^{p^e-1}$ は Z 上で 1 次独立である ([10, Lemma 2.1]). したがって $\mathrm{Hom}({}_{B^D}B_{B^D}, {}_{B^D}B_{B^D}) = Z[D] = Z \oplus ZD \oplus ZD^2 \oplus \cdots \oplus ZD^{p^e-1}$ となる.
(3) Δ を $\mathrm{Der}_{B^D}(B)$ の任意の元とする. (2) により, $\Delta = \sum_{k=1}^{p^e-1} z_k D^k$ $(z_k \in Z)$ と表される (Δ は定数項を持たないことに注意). 任意の $a, b \in B$ にたいして,

$$\begin{aligned}\Delta(ab) &= \sum_{k=1}^{p^e-1} z_k (\sum_{\nu=0}^{k} \binom{k}{\nu} D^{k-\nu}(a)D^\nu(b)) \\ &= \sum_{\nu=0}^{p^e-1} (\sum_{k=\nu}^{p^e-1} \binom{k}{\nu} z_k D^{k-\nu}(a))D^\nu(b)\end{aligned}$$

が成りたつ. 他方

$$\Delta(a)b + a\Delta(b) = (\sum_{k=1}^{p^e-1} z_k D^k(a))b + \sum_{\nu=1}^{p^e-1} a z_\nu D^\nu(b).$$

$1, D, D^2, \cdots, D^{p^e-1}$ は B 上1次独立である ([10, Lemma 2.1]) から,

$$az_\nu = \sum_{k=\nu}^{p^e-1} \binom{k}{\nu} z_k D^{k-\nu}(a) \ (a \in B, 1 \leq \nu \leq p^e - 1).$$

したがって,

$$\sum_{k=\nu+1}^{p^e-1} \binom{k}{\nu} z_k D^{k-\nu} = 0.$$

再び $1, D, D^2, \cdots, D^{p^e-1}$ は B 上1次独立であるから

$$\binom{k}{\nu} z_k = 0 \ \ (1 \leq \nu < k \leq p^e - 1).$$

よって [5, Theorem 3.1] の証明と同じ議論により, Δ が $ZD \oplus ZD^p \oplus \cdots \oplus ZD^{p^{e-1}}$ に属することがわかる. これで (3) の証明を終わる.
(4) は (1) と [7, Corollary 2.5] からただちに分かる.

REFERENCES

[1] K. Hirata, Some types of separable extensions of rings, *Nagoya Math. J.*, **33** 1968, 107–115.
[2] K. Hirata, Separable extensions and centralizers of rings, *Nagoya Math. J.*, **35** 1969, 31–45.
[3] K. Hirata and K. Sugano, On semisimple extensions and separable extensions overnon commutative rings, *J. Math. Soc. Japan*, **18** 1966, no. 2, 360–373.
[4] S. Ikehata, On separable polynomials and Frobenius polynomials in skew polynomial rings, *Math. J. Okayama Univ.*, **22** 1980, 115–129.
[5] S. Ikehata, Azumaya algebras and skew polynomial rings, *Math, J. Okayama Univ.*, **23** 1981, 19–32.
[6] S. Ikehata, A note on separable polynomials in skew polynomial rings of derivation type, *Math. J. Okayama Univ.*, **22** 1980, 59–60.
[7] S. Ikehata, On H-separable polynomials of prime degree, *Math. J. Okayama Univ.*, **33** 1991, 21–26.
[8] S. Ikehata and G. Szeto, On H-separable polynomials in skew polynomial rings of automorphism type, *Math. J. Okayama Univ.*, **34** 1992, 49–55.
[9] S. Ikehata and G. Szeto, On H-skew polynomial rings and Galois extensions, *Lecture Notes in Pure and Appl. Math.*, **159** Mercel Dekker, Inc., 1994, 113–121.
[10] S. Ikehata, Purely inseparable ring extensions and H-separable polynomials, *Math. J. Okayama Univ.*, **40** 1998, 55–63.
[11] S. Ikehata, Purely inseparable ring extensions and Azumaya algebras, *Math. J. Okayama Univ.*, **41** 1999, 63–69.
[12] S. Ikehata, On H-separable and Galois polynomials of degree p in skew polynomial rings, *Int. Math. Forum*, **3** 2008, no. 29-32, 1581-1586.
[13] S. Ikehata, On separable and H-separable polynomials of degree p in skew polynomial rings, *Int. J. Pure Appl. Math.*, **51** 2009, no.1, 149–156.
[14] S. Ikehata, A note on separable polynomials of derivation type, *Int. J. Algebra*, **3** 2009, no. 15, 707–711.
[15] S. Ikehata, On Hirata separable polynomials in skew polynomial rings, Submitted.
[16] K. Kishimoto, On abelian extensions of rings. I, *Math. J. Okayama Univ.*, **14** 1970, 159–174.
[17] K. Kishimoto, On abelian extensions of rings. II, *Math. J. Okayama Univ.*, **15** 1971, 57–70.
[18] K. Kishimoto, A classification of free quadratic extensions of rings, *Math. J. Okayama Univ.*, **18** 1976, 139–148.

[19] K. Kishimoto, A classification of free extensions of rings of automorphisim type and derivation type, *Math. J. Okayama Univ.*, **18** 1977, 163–169.

[20] Y. Miyashita, On a skew polynomial ring, *J. Math. Soc. Japan*, **31** 1979, no. 2, 317–330.

[21] T. Nagahara, On separable polynomials of degree 2 in skew polynomial rings, *Math. J. Okayama Univ.*, **19** 1976, 65–95.

[22] T. Nagahara, A note on separable polynomials in skew polynomial rings of atutomorphism type, *Math. J. Okayama Univ.*, **22** 1980, 73–76.

[23] T. Nagahara, Some H-separable polynomials of degree 2, *Math. J. Okayama Univ.*, **26** 1984, 87–90.

[24] T. Nagahara, A note on imbeddings of non-commutative separable extensions in Galois extensions, *Houston J. Math.*, **12** 1986, 411–417.

[25] G. Szeto and L. Xue, On the Ikehata theorem for H-separable skew polynomial rings, *Math. J. Okayama Univ.*, **40** 1998, 27–32.

[26] S. Yuan, Inseparable Galois theory of exponent one, *Trans. Amer. Math. Soc.*, **149** 1970, 163–170.

E-mail address: ikehata@ems.okayama-u.ac.jp